公的個人認証サービスを利用したデジタル遺品相続のオンラインサービスの提案

研究室 太田晃

平成 34 年 1 月 9 日

概要

様々なサービスがインターネットを通して利用することができるようになっている現在、デジタル遺品と呼ばれる個人が生前に利用していたデジタル機器に保存されたデータやインターネット上での登録情報の処理に対して、様々な問題が生じている。自身の死後のために財産処置の方法を残す手段として遺言書が存在するが、電子的な遺言書や電子的に相続を行うことのできるサービスは存在していない。その理由として、遺言書のデジタル化に伴う問題や個人の認証の問題が挙げられる。一般的な遺言書は民法上で、遺言者による「自筆」が要件になっており、スキャナで電子化してもデータの特性上、第三者の検証による遺言書の真正性の証明が難しいことがある。また、相続という重要な出来事において相続人であることを証明することは非常に重要なことであり強固な認証が必要となる。そこで本論文では、電子的な相続を実行するための要件を考察し、既存の制度の活用方法と新たなシステムの導入により電子的相続を実行するための仕組みを考案する。

1 研究背景

近年、デジタル遺品についての問題がしばしば登場するようになった。それは、パソコンやスマホといったデジタル機器の普及に伴い、持ち主が生前に利用していた機器内に保存されているデータ、また、インターネットを通じて利用していたSNSでのやりとりや暗号資産などの各種サービスに関するデータ、すなわちデジタル遺品が増加し、遺族はそれらのデータをどのように入手しどのように対処すべきなのかという問題に直面する場面が多くなったからである。

総務省の「令和 2 年通信利用動向調査」[1]によると、個人のインターネット利用状況が全体で 80%を越えており、年齢別にみても 6 歳から 69 歳までの各年齢層で 80%を越えているなど、幅広い層でインターネットが利用されていることが分かる。また、ソーシャルネットワーキングサービスの利用状況は全体で 70%を越えている。多くの個人に利用されているこれらのデジタル機器の中には当然様々なデータが存在しているため、デジタル遺品に関するトラブルが起きる可能性は十分に高いと考えられる。現在の個人のインターネット利用状況やソーシャルネットワークサービスの利用状況では、高齢者の利用状況が約 50%であるが、今後さらに利用割合が増加することが容易に考えられる。ここで、個人の利用者が死亡した場合、それまで故人が利用していたSNSアカウントやその他サービスのアカウントなどが長期間放置されたままの状態になってしまう。そうなると、SNSの場合はアカウントが乗っ取られて故人の名誉を傷つける恐れがあったり、悪用される可能性が高まったりする。また、「令和 2 年通信利用動向調査」[1]によると、ソーシャルネットワークサービスの利用目的として約 90%が「従来からの知人とのコミュニケーションのため」と回答しているように、今や SNS はコミュニケーションのためのツールとして利用することが一般的であり、実際に会ったこ

とはないがSNS上だけでつながっている友人がいるという人も少なくない。
このような場合、利用者が亡くなったことを知らせたり、生前にどのようなつながりがあったのかを調べるために遺族が故人のSNSアカウントを利用することは有用である。しかし、利用者が亡くなるとたとえ遺族であってもそのアカウントを操作して何らかの情報を得るということは困難である。実際、主要なSNSの1つである「Twitter」では、ユーザが亡くなった場合は故人との関係を証明したうえで権限のある遺産管理人または故人の家族とともにアカウントを停止、削除することはできるが、故人のアカウントのログイン情報の開示やそのアカウントを操作するといったことは、故人との関係によらず行うことができない。また、その他のサービス、特にFX取引や暗号資産、有料会員サービスなどのお金に関連するサービスのアカウントが放置され、遺族に追加請求されるといった事例が存在する。さらに暗号資産に注目してみると放置による知らないうちに発生する被害だけでなく、相続をするときに被相続人が暗号資産を保持していたことが確認できても秘密鍵や秘密鍵を含むパスワードを知らなかった場合、実際にはその暗号資産の送金処理を行うことができないにも関わらず相続税は課税されてしまう。秘密鍵などに関して「知らない」「忘れた」ということを証明することができないからである。これらの問題を引き起こさないようにするために生前に相続人となりうる人物に周知してもらうことや死後どのようにそれらを処理すべきかといった「遺言」が重要になってくる。自筆証書遺言書保管制度という法務局によって自筆遺言書を管理・保管してくれるサービスがはじめられた。しかし、電子的な遺言書を残しオンライン上で相続をすることができる仕組みは存在していない。これには、電子的な遺言書が認められていないことや被相続人の死亡確認及び相続人の本人確認をオンライン上で行う仕組みが利用されていないことが関係している。遺言書民法において本文全体、氏名及び日付を自筆し、押印しなければならなくワープロなどにより電子的に作成された遺言書は有効としないとされている。これは筆跡や氏名をもとに遺言書作成者を特定するためである。つまり、遺言書の作成者を特定することが可能であるならば電子的な遺言書でも効力を認められてもよいのではないかと考える。そこで、本論文ではオンライン上での相続サービスに必要な仕組み、制度を考察し、それをもとにどのようなシステムであれば電子的な相続として成立するのかということを考案する。

2　関連技術と問題点

2.1　デジタル遺品の問題点

通常、遺品の相続人に当たる人物が機器内に残されたデータや機器そのものを元に、相続するためのものや連絡のための交友関係の把握のために手がかりを探し始める。しかし、機器内には多くの情報が蓄積されているため機器そのものが複数の相続人による共有の状態になり、ロック解除のために他の相続人の了解をとる必要があるなど手間がかかることがある。ただ、多くの場合においてログインのためのIDやパスワードと言った情報が分からず、デジタル機器そのものへのアクセスをすることができない。そこで、デジタル機器のロックを解除するためにパスワードの解析を行ってくれる業者にお願いして、機器のロックを解除しようとするが必ずしもパスワードの解析が成功するわけではないし、仮にパスワードが判明、もしくは事前に知っていて機器のロックを解除することに成功し、その機器で故人がどのようなサービスを利用していたかを知ることができたとしても、そのサービスで利用していたアカウントへのログインのための情報が分からず、結局はどのようなやり取りが行われていたかやどのような資産が管理されていたかを知ることは非常に難しい。故人が利用していたサービスが判明すれば、そのサービスの運営サイトを訪れ、相続の手続きを行うことができるかもしれないが、多くの場合そのためには正当な相続人であることを証明する必要があり、そのために死亡証明書や戸籍情報などの紙媒体の情報を郵送するなどまた、SNSを含めた多くのサービスは基本的にアカウント自体の相続を利用規約により禁止している場合が多

く、いくら正当な相続人であっても利用規約違反になることがあるなど規制が多い。

2.2 相続

2.3 遺言書

普通方式遺言書には、大きく分けて「自筆証書遺言」、「公正証書遺言」、「秘密証書遺言」の3種類があり、本稿で注目すべきものは、「自筆証書遺言」である。2020年7月10日に法務局による遺言書の預かりサービスとして「自筆証書遺言書保管制度」が開始された[2]。しかし、この制度で預かりが可能なのは「自筆証書遺言」であり、その名の通り「自筆」であることが重要視されている。民法第968条1項により「自筆証書によって遺言をするには、遺言者が、その全文、日付及び氏名を自書し、これに印を押さなければならない。」と記されている。しかし、2019年1月13日に施行された民法第968条の改正により、遺言書の財産目録についてはワープロ等の作成が認められ自筆である必要がなくなったが、依然として遺言書の本文は自筆しなければならない。なぜこれほど自筆が重要視されているのかというと、遺言は、相続をめぐるトラブルを防止するために有用な手段であり、特に自筆証書遺言は自筆さえできれば遺言者本人のみで作成が可能であり、証人が不要であるなどコストが低くく手軽に作成できる反面、遺言書の変造や偽造がなされる可能性が高く、それらが疑われたときに本当に遺言者が作成したものであるかどうかを遺言者の筆跡を元に鑑定するためである。また、「日付及び氏名を自書し、これに印を押さなければならない。」とあり、日付の記載により、遺言書が複数発見された場合、どちらがより後に作成されたものであるかの判断を可能にし、その日付における遺言者の遺言能力の有無を判断するために利用される。遺言書に署名する氏名としては、遺言者の特定のために原則として戸籍上の本名を書かなければならないが、「遺言者」を特定できるのであれば芸名やペンネームなどの本名以外の記載であっても有効性が認められる場合[3]が存在したり、日付及び氏名に押す「印」については特別な定めが存在しないので実印である必要がなく、指印でも有効性が認められる場合[4]が存在する。しかし、「指印」による押印や押印の代わりに「花押」を書くことでは民法968条の要件を満たさないとして有効性が認められない場合[5][6]も存在する。これらの有効になった事例と無効になった事例に共通している判決理由の元になっている考えとして、自筆による遺言書の方式として自書のほかに押印を必要としたのは、遺言の全文の自書と押印によって遺言者の同一性や真正性を確保するとともに、重要な文書は作成者による署名と押印をすることで文書の作成を完結させるということが通例であり法に照らし合わせても文書の完成を担保するものであるということがある。つまり、遺言者本人が正式に作成したものであることを確認することが出来るなら有効となり、確認することができないのならば無効になることが分かる。

2.4 公開鍵暗号

本稿での公開鍵暗号とは公的個人認証サービスにおいて用いられている暗号方式であるRSA暗号のことを指すものとする。公開鍵暗号では、公開鍵と秘密鍵の2つの鍵を1組のペアとして扱う。一方の鍵でメッセージの暗号化を行うと、他方の鍵でのみ復号可能である。その名の通り公開鍵は他者に知られることを前提にしているのに対し、秘密鍵は絶対に他者に知られてはいないことを前提としている。それは、公開鍵からは秘密鍵を作成できないのに対して、秘密鍵から公開鍵を作成することができ、一般に利用する際には、公開鍵で暗号化したメッセージを復号するためにはそれに対応した秘密鍵を用いるためである。万が一、暗号化したメッセージが第三者に入手されたとしてもその公開鍵に対応する秘密鍵を知らなければそのメッセージを解読することができず、メッセージの漏洩を防ぐことができる。もし、秘密鍵が他者に漏洩してしまうとせっかく公開鍵を用いて暗号化したメッセージであっても他者に知られてしまう恐れがある。

2.5　電子署名

紙文書でのやりとりの際には印鑑やサインを利用して、その文書が正当な人物や組織により作成され、改ざんもされていないということを証明していた。しかし、電子文書においては文書にペンで直接サインや押印をすることはできず、サインをして押印したものをスキャナで取り込んだとしても、電子データの特性上簡単にコピー&ペーストすることが可能であるため正当な人物により作成されたものであることやそれが改ざんされていないことを証明することはできない。電子署名及び認証業務に関する法律 (電子署名法) では同一の法的拘束力が認められているものとして電子サインと電子署名がある。電子サインはタッチペンなどを用いて電子的にサインするものであり、手軽に利用できるものであり、対面であれば目の前にいる相手が契約書にサインする人物であるということが判断できるため有用である。しかし、対面でなければ実際に電子サインをした人物と本来の契約者が同一の人物であるということを電子サインから判別することは困難であるため、対面でないサービスでの本人確認に利用するには信頼性が低い。電子署名は、紙文書へのサイン、押印といった真正性の証明を電子文書上で実現するための技術である。つまり、電子署名を電子文書に付与することにより、文書の改ざんやなりすましを検出することができ、その文書が原本であることが証明できる。電子署名を付与するためには、公開鍵暗号でも説明した、公開鍵と秘密鍵のペアを利用する。文書の送信者は、自身の秘密鍵を用いて文書に署名を施す。受信者は、受け取った文書が本当に送信者によって署名されたものであるかを送信者の公開鍵を用いて検証する。検証に成功すればその文書は真に送信者が作成したものであり改ざんされていないことも確認できる。つまり、電子署名には電子版の印鑑証明書に相当する電子証明書が用いられており、複製も所有者以外の使用もできないため対面でないサービスでの本人確認での利用においても高い信頼を発揮することできる。

2.6　電子証明書

電子署名が施された文書の署名検証を行うとき送信者の公開鍵を用いるのだが、その公開鍵が本当に送信者のものであるかという証明ができない。そこで、「この公開鍵の持ち主は送信者で間違いない」と保証してくれるものが電子証明書となる。電子証明書を信頼するべきか否かを判断する規準として、電子証明書にはその電子証明書の発行者や有効期間、公開鍵の所有者の情報などが記載されており、信頼できる第三者 (認証局) によって電子署名がなされている。認証局とは、認証業務運用規定やプライバシーポリシーなどを公開し、信用できることを公に認められている機関であり、公的個人認証サービスにおいては、地方公共団体情報システム機構 (J-LIS) が認証局の役割を務めている。

2.7　公的個人認証サービス

公的個人認証サービスとは、オンラインでの申請や届け出といった行政手続きやインターネットサイトへのログインを行う際に用いられる本人確認の手段である。本人確認には、マイナンバーカードに搭載されている電子証明書を利用する。マイナンバーカードに搭載される電子証明書は地方公共団体情報システム機構 (J-LIS) により発行されており、マイナンバーカードは耐タンパー性を有しているため、マイナンバーカード内の情報が不正に読みだされたり解析されようとした場合、その内容が自動的に消去される等の対抗措置が講じられているので高いセキュリティ性を確保している。このマイナンバーカードに搭載されている電子証明書を読み取り、これを利用して電子署名やユーザ認証を行うことができる。公的個人認証サービス自体は、マイナンバー制度が開始される以前、2004 年 1 月 29 日に個人向けのサービスとして電子証明書の発行が開始されたが、これは、オンラインで行政機関への届け出などを行った人物が本当に住民基本台帳に記録されている人物であるかを確認する仕組みであり、住民基本台帳ネットワークシステムとして存在していた。このシステムでの公的個人認証サービ

スを利用するためには、住所地市町村に申請して住民基本台帳カードを交付してもらい、そのICチップに電子証明書と秘密鍵を格納する必要があった。以前の公的個人認証サービスによる電子証明書や電子署名の利用は、行政手続きをオンラインで行う場合にのみ利用可能であった。しかし、2013年5月31日に公布された社会保障・税番号制度関連四法によって、公的個人認証法の一部が改正[7]され、公的個人認証サービスの利用範囲が変更された。電子証明書の発行者が都道府県知事からJ-LISに変更され、「利用者証明用電子証明書」という電子証明書の新設がなされた。さらに、全国民に個人番号が付番されることとなり、2016年1月から住民基本台帳に記録されている者に対し、その者の申請により、個人番号カードが交付されるようになりそれに伴い、住民基本台帳カードの発行が終了するため、電子証明書格納媒体が住民基本台帳カードからマイナンバーカードに変更された。加えて、民間事業者においても電子署名や電子証明書による本人確認サービスが利用可能になった。この業務のことを特定認証業務といい、2016年1月より、総務大臣による認定を受けた民間企業は総務大臣認定事業者となりマイナンバーカードの電子証明書の署名検証・利用者証明検証業務を行うことが可能になった。2021年12月時点での総務大臣認定事業者は16社である。

2.8 公的個人認証サービスにおける電子証明書

現在の公的個人認証サービスでは、二種類の電子証明書が標準的に提供されている。署名用電子証明書と利用者証明用電子証明書の2つである。署名用電子証明書と利用者証明用電子証明書の違いは、その利用用途と個人情報の基本となる氏名、性別、住所、生年月日の4つの情報である基本四情報の記載があるか否か、そして失効条件である。これらの証明書の使用用途は以下の通りである。

- 署名用電子証明書
  電子文書を行政機関に提出するための署名や捺印に相当するものとして署名用電子証明書を利用して電子申請を行う。具体的には、e-Taxの電子申請を行うために利用される。電子文書を作成・送信した者が利用者本人であり、文書が改ざんされていないことを確認するために用いられる。ICカードの紛失をしたために電子証明書の失効申請をしたり、有効期間が満了したり本人が死亡した場合に加えて、住民票の基本四情報の記載が修正された場合に失効する。基本四情報が記載されている。

- 利用者証明用電子証明書
  インターネット上のサービスを利用する際に利用しているのが本人であることを証明するための手段として用いられる。具体的には、マイナポータルへのログインやコンビニでの住民票の交付などの公的な証明書の交付サービスのために用いられる。ICカードの紛失をしたために電子証明書の失効申請をしたり、有効期間が満了したり本人が死亡した場合に失効する。基本四情報は記載されていない。

2.9 公的個人認証サービスにおける電子証明書の検証

電子証明書の署名検証の実施をする場面として、利用者が行政機関などに文書を提出した際に行政機関側が受け取った利用者の電子証明書の検証をする場面と行政機関から個人あてに返却された文書の電子証明書を検証する場面である。
利用者の電子証明書を検証が可能であるのは、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（公的個人認証法）の第十七条に記載されている、行政機関、裁判所と特定認証業務を行う民間事業者のうち内閣総理大臣や総務大臣による認定を受けた民間事業者である。電子証明書の失効条件は先述の通りである。失効しているかを確認する方法は2つある。

- CRL(Certificate Revocation List) 認証局から定期的に証明書のシリアル番号

とその証明書の失効情報 (有効期限よりも前に何らかの理由で失効したもの) のリストである CRL が配布され、それをダウンロードしてシリアル番号を照会して検証する。1 つの証明書を検証するためにも CRL 全体をダウンロードする必要がある。

- OCSP(Online Certificate Status Protocol) CRL の代替として策定されたものであり、OCSP レスポンダと呼ばれるサーバを稼働させ、そこで CRL を保管する。検証者は OCSP レスポンダに対して証明書のシリアル番号をもとに有効性の照会、署名付きの応答で有効性の検証を行う。電子証明書を個別に検証可能である。しかし、検証数が多くなると通信回数が多くなってしまう。

2.10 マイナンバーカード

マイナンバーカードとは、マイナンバーを保有する住民が申請すると無料で交付されるプラスチック製のカードであり、カード内に IC チップを搭載している。この IC チップ内に公的個人認証サービスで用いることができる電子証明書が搭載されており、公的な身分証明書としても利用できる IC カードである。マイナンバーカードの電子証明書の利用にはマイナンバーの使用はされていないため、番号法にふれることなく民間事業者を含めた様々な事業者が多様な用途に利用可能である。

2.11 マイナンバーカードのアプリ

マイナンバーカードの IC チップには以下の 4 つのアプリケーションがある。

- 券面アプリケーション (券面 AP)
- 公的個人認証サービスによる電子証明書アプリケーション (JPKI-AP)
- 券面事項入力補助アプリケーション (券面入力補助 AP)
- 住基アプリケーション (住基 AP)

券面 AP と券面入力補助 AP は主に対面による記載内容の確認の際に記載内容が改ざんされていないか確認したり、事務作業のためにテキストデータとして利用する際に使用される。ただし、番号法に基づく事務でのみ利用可能である。JPKI-AP は先述した署名用電子証明書と利用者証明用電子証明書を利用する際に使用される。住基 AP は住基ネットの事務のために住民票コードをテキストデータとして扱う際に使用される。これらの利用のためには多くの場合において、4 桁もしくは 6~16 桁の暗証番号の入力が必要であり規定回数の誤入力によりパスワードロックがかかってしまい、解除には市町村窓口での申請が必要となる。

2.12 タイムスタンプ

タイムスタンプとは、デジタルデータがその日時において存在していたことを証明し (存在証明)、その日時以降にデータが変更されていないことを証明する技術である。タイムスタンプを発行してもらうにはタイムスタンプサービスの信頼の基盤でもある時刻認証局 (Time-Stamping Authority) に特定のデータを送付する必要がある。送付するデータはメッセージダイジェストと呼ばれる、タイムスタンプを付与する元のデータのハッシュ値である。これを受け取った TSA はこのハッシュ値に時刻情報を偽造できないようにして結合したタイムスタンプトークンを送信者に送付することによりタイムスタンプを発行する。このときに付与されたタイムスタンプを検証するには TSA に送信した元のデータのハッシュ値を計算し、TSA により付与されたタイムスタンプに含まれているハッシュ値とを比較して、一致しているかを確認する。電子帳簿保存法においてタイムスタンプの付与されたデータの信頼性を担保し、改ざん防止の役割を担っている。

3　公的個人認証サービスを利用したデジタル遺品相続サービス

本章では、本論文で提案する公的個人認証サービスを利用したデジタル遺品相続サービスについて述べる。

3.1　相続を電子化する上での問題

本研究では、相続を電子化する上での問題点として4点を取り上げる。遺言書の真正性の証明と被相続人の死亡確認、相続人の本人確認性、そしてデジタル遺品特有である暗号資産の不正送金による問題である。

第2章でも述べたが、一般的に遺言書は日付及び氏名を自筆し、押印をすることが要件とされている。しかし、要件を満たした紙の遺言書をそのままスキャナで電子化したとしても有効な遺言書とは認められない。その理由としては、遺言書の筆跡や押印により真正性の証明を行うためである。つまり、電子化した遺言書を有効にするためにはその真正性を確認できることが求められる。

また、相続とは被相続人が亡くなった後に開始されるものであり、被相続人が生存している間は相続が発生してはいけない。電子的に死亡確認をする方法として一般的なものは存在しない。あるサービスを長期間利用していないことやSNSなどによる死亡報告をもって死亡とするのは信憑性があまりにも乏しい。信頼できる機関である行政機関による報告などの信頼性のある確認が必要である。

相続人になりうる人物は基本的には親族であり、対面で相続を行う場合は相続人本人であることを確認することは容易である。しかし、電子的に行う場合、特に相続という重要な場面においての本人確認は強固な確認が必要である。

通常、暗号資産はアドレスの管理者が保持しているアドレスに対応する秘密鍵を利用することで送金処理を完了することができる。しかし、暗号資産を相続するとなると管理者であった被相続人は死亡しているため暗号資産の相続を行う際に被相続人が関与することはできない。暗号資産の相続を行うときに被相続人が保持していた秘密鍵を使用せずとも送金を可能にする必要がある。

3.2　問題解決へのアプローチ

上記で述べた問題に対し、本論文では、公的個人認証サービスを利用したデジタル遺品相続サービスを提案する。本手法は、真正性や本人確認性に対する問題に対して公的個人認証サービス、不正送金対策に暗号資産で利用されている技術を用いることで前述の問題の解決を目指す。本提案手法の機能要件を次項に示す。

3.2.1　遺言書の真正性、本人性確認

電子化された遺言書の問題の解決には、抜本的には民法を改正する必要があるが、電子化された遺言書の真正性を証明することにより解決される。遺言書を登録する際には、登録者とサービス提供者間で遺言書のやり取りを行う必要がある。しかし、その遺言書は本当にその登録者が作成したものであり、遺言書作成時以降に誰にも改ざんがなされていないものであるという保証はない。そこで、本提案手法では電子署名に利用する公開鍵・秘密鍵のペアに公的個人認証サービスを利用する。公的個人認証サービスで提供されている署名用電子証明書を利用して署名を行うことにより、J-LISによって認証されている鍵ペアを利用することができ、遺言書の真正性がJ-LISによって保証される。また、公的個人認証サービスで提供されている利用者証明用電子証明書を利用することにより、相続人の本人性確認がJ-LISによって担保される。

3.2.2　死亡確認

相続の開始は登録者 (被相続人) の死亡が確認されたことによって開始されるべきであり、死亡の確認がなされていないのに、

3.2.3 暗号資産の不正送金

4 提案手法

4.1 サービスの設計

相続の執行人となるサービス提供機関：相続という重要な出来事を執行する立場になる以上、法的な規制も厳しく、相当な信頼性がなければ利用者は安心してサービスを利用することはできない。そのため、サービスを行うのは一般企業では不適当である

参考文献

[1] 総務省. 令和 2 年通信利用動向調査. https://www.soumu.go.jp/johotsusintokei/statistics/data/210618_1.pdf

[2] 自筆証書遺言書保管制度のご案内. https://houmukyoku.moj.go.jp/mito/page000001_00041.pdf

[3] 裁判所の判例として大阪高裁昭和６０年１２月１１日が挙げられているが見つけられていない. https://www.mc-law.jp/sozokuigon/23683/

[4] 遺言無効確認請求事件. https://www.courts.go.jp/app/files/hanrei_jp/210/052210_hanrei.pdf

[5] 遺言書真否確認請求事件. https://www.courts.go.jp/app/files/hanrei_jp/310/020310_hanrei.pdf

[6] 遺言書真正確認等，求償金等請求事件. https://www.courts.go.jp/app/files/hanrei_jp/930/085930_hanrei.pdf

[7] 総務省. 公的個人認証サービス利用のための民間事業向けガイドライン. https://www.soumu.go.jp/main_content/000400619.pdf

[8] 地方公共団体情報システム機構. 公的個人認証サービスポータルサイト. https://www.jpki.go.jp/procedure/period.html

[9] マイナンバー制度とマイナンバーカード. https://www.soumu.go.jp/kojinbango_card/03.html